AMENDMENTS

In the Claims

The following is a marked-up version of the claims with the language that is underlined ("___") being added and the language that contains strikethrough ("——") being deleted.

1.   (Currently Amended) A method for transparent file proxying, the method comprising:

coupling a plurality of computing devices to a local area network, each of ~~at least one of~~ said plurality of computing devices including ~~an ability to route communication packets to said remaining plurality of computing devices, each of said plurality of computing devices including~~ a local memory element containing a plurality of files~~,~~ ~~coupling said~~ at least one of said plurality of computing device coupled to a wide area ~~communication~~ network;

coupling a remote memory element to said wide area network, said remote memory element configured to maintain a copy of the first file selected from said plurality of files contained in the local memory elements of said plurality of computing devices;

said at least one of said plurality of computing devices to a wide area communication network;

coupling a remote computing device to said remote memory element~~,~~;~~said remote memory element configured to maintain a copy of a first file selected from said plurality of files contained in the memory elements of said plurality of computing devices if a first user of the remote computing device is authorized access to the first file~~;

intercepting, in said remote memory element, an Internet Protocol (IP) communication message from said remote computing device, said IP communication message corresponding to a request from ~~the~~ a first user to access ~~said first~~ a requested file; and

providing <u>information corresponding to</u> said copy of said first file to said remote

computing device <u>from said remote memory element without</u> ~~when said remote memory~~

~~element intercepts~~ said IP communication message ~~from said remote computing device if said~~

~~IP communication message requests said first file from one of said plurality of computing~~

~~devices connected to said local area network, thus providing said copy of said first file to said~~

~~remote computing device without said IP communication message~~ traversing said wide area

communication network and <u>said local area network if the first user is authorized to access</u>

<u>said requested file and if said requested file corresponds to said first file.</u>

2.   (Currently Amended) The method of claim 1, wherein said at least one of said

plurality of computing devices periodically updates said ~~selected~~ <u>copy of said first</u> file

maintained in said remote memory element.

3.   (Currently Amended) The method of claim 1, wherein said ~~selected~~ <u>copy of</u>

<u>said first</u> file is chosen to be maintained in said remote memory element based upon ~~any~~ <u>at</u>

<u>least one</u> of a plurality of policies, <u>wherein said plurality of policies are chosen from the</u>

<u>group consisting of user policies, group policies and corporate policies</u>.

4.   (Canceled)

5.   (Currently Amended) The method of claim 1, wherein<u>, if the first user is</u>

<u>authorized access,</u> said remote memory element updates said ~~selected~~ <u>copy of said first</u> file <u>in</u>

<u>response to receiving information corresponding to a modification of said first file from said</u>

<u>remote computing device</u> ~~and causes a file located in said plurality of files and corresponding~~

~~to said selected file to be updated~~.

6.   (Currently Amended) A system for transparent file proxying, comprising:

a local network to which is coupled a plurality of computing devices, at least one of said plurality of computing devices including the ability to route communication packets to said remaining plurality of computing devices, each of said plurality of computing devices including a memory element containing a plurality of files;

a communication network coupled to said at least one of said plurality of computing devices;

a remote memory element coupled to said communication network;

a remote computing device connected to said remote memory element, said remote memory element configured to intercept an Internet Protocol (IP) communication message from said remote computing device, said remote memory element configured to maintain a copy of a first file selected from said plurality of files contained in the memory elements of said plurality of computing devices ~~if a first user of the remote computing device is authorized access to the first file~~; and

wherein said remote memory element is configured to provide <u>information corresponding to</u> said copy of the first file to said remote computing device ~~when~~ <u>in response to</u> said remote memory element<u>:</u>

~~intercepts~~ <u>intercepting</u> said IP communication message from said remote computing device,

determining that the first user is authorized access, and

determining that said file corresponds to said first file,

said IP communication message corresponding to a request from the first user to access said first file from one of said plurality of computing devices connected to said local network, thus providing <u>information corresponding to</u> said copy of the first file to said remote computing device without said IP communication message traversing said communication network and said local area network.

7.   (Currently Amended) The system of claim 6, wherein said at least one of said plurality of computing devices periodically updates said selected file maintained in said remote memory element.

8.   (Currently Amended) The system of claim 6, wherein said ~~selected~~ copy of said first file is chosen to be maintained in said remote memory element based upon ~~any~~ at least one of a plurality of policies, wherein said plurality of policies are chosen from the group consisting of user policies, group policies and corporate policies.

9.   (Canceled)

10.   (Currently Amended) The system of claim 6, wherein, if the first user is authorized access, said remote memory element updates said ~~selected~~ copy of said first file in response to receiving information corresponding to a modification of said first file from said remote computing device ~~and causes a file located in said plurality of files and corresponding to said selected file to be updated~~..

11. – 19.   (Canceled)

20.   (New) The method of claim 5, wherein, after the remote memory device updates said copy of said first file, said remote memory device causes said first file to be updated.

21.   (New) The method of claim 1, wherein, in determining whether the first user is authorized access to said file, if the user is authorized access to said file but a copy of said file

is not stored locally by said remote memory device, said remote computing device forwards said IP communication message via said wide area communication network and said local area network such that said remote computing device is able to retrieve a copy of said first file.

22.   (New) The system of claim 6, wherein, in determining whether the first user is authorized access to said file, if the user is authorized access to said file but a copy of said file is not stored locally by said remote memory device, said remote computing device forwards said IP communication message via said wide area communication network and said local area network such that said remote computing device is able to retrieve a copy of said first file.

23.   (New)The method of claim 1, further comprising:

preventing the user from obtaining information corresponding to said file from said remote memory element if the user is not authorized access to said file.